# Controlled Doping via High-Order Rootchecks in Graph Codes

Joseph J. Boutros
Texas A&M University at Qatar
Education City, 23874, Doha, Qatar
boutros@tamu.edu

***Abstract*—Code construction for a data transmission channel with a limited number of degrees of freedom is a big challenge. For codes on graphs, a solution based on rootchecks has been proposed [1]. In this paper, we start by establishing a new proof for full diversity equivalence between the block-fading and the block-erasure channels. Then, we show how doping [2] can be made via high-order rootchecks. This controlled doping will help in increasing the diversity order of parity bits while boosting the coding gain of information bits in full-diversity root-LDPC codes. New ensembles of root-LDPC codes are designed such that 100% of parity bits achieve full diversity.**

## I. Introduction

Consider a data transmission channel with a limited number of degrees of freedom. A transmitted codeword can be divided into $B$ blocks where each block is observing a different channel state. For a given signal-to-noise ratio, it is not possible to guarantee a vanishing error probability at asymptotic code length; Shannon capacity of such a non-ergodic channel is zero [3]. We restrict our study to the worst case $B = 2$ channel states. As an example, the block-fading channel with binary input and additive white Gaussian noise is defined by

$$y_n = \alpha_1 \cdot x_n + \eta_n, \quad \text{for} \quad n = 1 \ldots \frac{N}{2}, \tag{1}$$

$$y_n = \alpha_2 \cdot x_n + \eta_n, \quad \text{for} \quad n = \frac{N}{2} + 1 \ldots N. \tag{2}$$

The code length is $N$ bits, symbols $x_n \in \{-1, +1\}$, the additive noise is $\eta \sim \mathcal{N}(0, \sigma^2)$, signal-to-noise ratio is $\gamma = \frac{1}{2\sigma^2}$ (here $\gamma = E_s/N_0$ is a signal-to-noise ratio per symbol), and the two fading coefficients are independent and identically distributed, $\alpha_i \in \mathbb{R}^+$. The fading distribution tail satisfies $p(\alpha_i^2) \approx 1$ for $\alpha_i^2 \ll 1$. The all-zero codeword is assumed to be transmitted and the value of fading coefficients is perfectly known by the decoder. For a given fading $\alpha \in \mathbb{R}^+$ and a channel output $y$, when no *a priori* information is available, the log-likelihood ratio required for iterative probabilistic decoding is

$$\begin{aligned} \Lambda &= \log\left(\frac{p(x=+1|y,\alpha)}{p(x=-1|y,\alpha)}\right) = \log\left(\frac{p(y|x=+1,\alpha)}{p(y|x=-1,\alpha)}\right) \\ &= \frac{2\alpha y}{\sigma^2} \propto (\alpha^2 + \alpha\eta). \end{aligned} \tag{3}$$

The case $\alpha_1 = \alpha_2$ corresponds to a binary-input Gaussian channel, i.e. $\Lambda = \alpha + \eta$ after division by the constant fading coefficient. This case is equivalent to the study of an ergodic channel without fading ($\alpha_1 = \alpha_2 = 1$). For $\alpha_1 \neq \alpha_2$, it is not possible to divide the message $\Lambda$ by $\alpha$. Thus, in the general case, after rewriting $\alpha\eta$ as $\eta$, a message at the decoder input would be expressed as $\alpha_1^2 + \eta_1$ and $\alpha_2^2 + \eta_2$ for the first half-codeword and the second half-codeword respectively.

For any finite non-zero value of $\gamma$, according to (3), a zero fading $\alpha = 0$ is equivalent to a zero message $\Lambda = 0$, and an infinite fading $\alpha = +\infty$ is equivalent to a full-confidence message $\Lambda = +\infty$.

If Min-Sum decoding is applied on an LDPC code, instead of Belief Propagation [4][5], messages propagating along graph edges would always be expressed as

$$\Lambda = \xi\alpha_1^2 + \zeta\alpha_2^2 + \eta, \tag{4}$$

for any number of decoding iterations, where $\xi$ and $\zeta$ are integers representing the energy coefficients for both fading states. On the other hand, a maximum likelihood (ML) decoder maximizes the correlation metric

$$\alpha_1 \sum_{n \leq N/2} y_n x_n \; + \; \alpha_2 \sum_{n > N/2} y_n x_n. \tag{5}$$

As shown in [1], a code construction for ML decoding is not necessarily suitable for iterative decoding. Let $P_e$ denote the error probability after decoding, for a given type of the LDPC decoder. The diversity order attained by an error-correcting code for channel (1)&(2) is defined as [3]

$$d = -\lim_{\gamma \to +\infty} \frac{\log(P_e)}{\log(\gamma)}. \tag{6}$$

The error probability before decoding on channel (1)&(2) is $P_0 \propto 1/\gamma$, for $\gamma >> 1$. For a general channel with an uncoded error probability $P_0 \propto 1/\gamma^{d_0}$, the state diversity order [6] for a code construction is

$$d_s = +\lim_{\gamma \to +\infty} \frac{\log(P_e)}{\log(P_0)}, \tag{7}$$

and the total diversity order becomes $d = d_s \times d_0$. Unless otherwise stated, we assume that $d_0 = 1$ and $d = d_s$.

*Definition 1:* Given a decoding algorithm and a non-ergodic channel with $B$ states, a code construction is said to be *full-diversity* (FD) if the attained diversity order is $d = B$.

For $B = 2$, the aim of code constructions in [1][2] was to build full-diversity low-density parity-check codes at the maximum coding rate $1/2$, a construction leading to an ensemble referred to as root-LDPC codes. Examples of rate-$1/3$ full-diversity root-LDPC codes for $B = 3$ and rate-$1/2$ maximum-diversity root-LDPC codes for $B=4$ can be also found in [1] and [2] respectively.

It is unclear from (6) and Definition 1 whether diversity order $d$ and its full-diversity property are defined for the bit error probability $P_{eb}$ or the word error probability $P_{ew}$! For a code length $N < +\infty$, we have $P_{eb} \leq P_{ew} \leq NP_{eb}$. If $\log(N) = o(\log(\gamma))$ then $P_{eb}$ and $P_{ew}$ have an identical diversity order. For simplicity, assuming that $N$ is finite or increasing logarithmically with signal-to-noise ratio, we will write $P_e$ to denote both bit and word error probabilities. Usually, $P_e$ would represent $P_{eb}$ when dealing with iterative decoding and it refers to $P_{ew}$ in ML decoding.

In the next section, we describe the erasure channel approach for designing root-LDPC codes and we prove the FD-equivalence between block-erasure and block-fading channels. Diversity population evolution [2] is restated in section III and doping of parity bits is studied. Section IV introduces different code constructions for controlled doping. The paper ends with experimental results of root-LDPC codes on fading channels and the conclusions.

## II. The Erasure Channel Approach for Non-Ergodic Fading Channels

The channel model is a binary-input real-output channel as defined in (1)&(2). Consider a linear binary code $\mathcal{C}[N,K]$ of dimension $K$, length $N$, and coding rate $K/N \leq 1/2$. Under ML decoding, the pairwise error probability between the $0$ codeword and a non-zero codeword $c$ can be upper bounded by [7][8]

$$P(0 \to c) \leq \frac{1}{(1+\omega_1(c)\gamma)} \times \frac{1}{(1+\omega_2(c)\gamma)}, \qquad (8)$$

where $\omega_1(c)$ is the Hamming weight of the first $N/2$ bits in $c$ and $\omega_2(c)$ is the Hamming weight of the last $N/2$ bits in $c$. In our convention, the Hamming weight is equal to the number of '+1' symbols in the transmitted codeword $x(c) = (x_1, x_2, \ldots, x_N)$, $x_n$ being the channel input at time instant $n$ as defined in (1)&(2).

*Lemma 1:* Under maximum-likelihood decoding, full diversity on the block-fading channel is achieved if and only if $\omega_1(c) \neq 0$ and $\omega_2(c) \neq 0$ for all non-zero codewords $c \in \mathcal{C}[N,K]$.

*Proof:* Assume there exists a codeword $c$ such that $\omega_1(c) \neq 0$ and $\omega_2(c) = 0$. Then, (8) and the Union bound tell us that $d \geq 1$. Using this same codeword, we can write a lower bound for the total error probability as follows

$$\begin{aligned} P_e &\geq P(0 \to c) = E_{\alpha_1}\left[Q(\sqrt{2\gamma\omega_1\alpha_1^2})\right] \\ &\geq P(\alpha_1^2 \leq \alpha_0^2) \cdot Q(\sqrt{2\gamma\omega_1\alpha_0^2}) \qquad (9) \\ &\geq \frac{1}{\gamma} \cdot Q(\sqrt{2\omega_1}) + o(\frac{1}{\gamma}). \qquad (10) \end{aligned}$$

Hence, $P_e$ has diversity order $d \leq 1$. This proves that $d = 1$. Similar reasoning is made for $\omega_1(c) = 0$ and $\omega_2(c) \neq 0$. Inequality (9) is found by splitting the integral $\int_0^{\infty} = \int_0^{\alpha_0^2} + \int_{\alpha_0^2}^{\infty}$, and (10) is found by taking $\alpha_0^2\gamma = 1$. The function $Q(x)$ is the standard Gaussian tail function.

Now let us assume that $\omega_1(c) \neq 0$ and $\omega_2(c) \neq 0$, then from (8) we get that $d \geq 2$. Since the channel has $B=2$ states, we know that $d \leq B$ [3], so $d=2$. We can also lower bound $P_e$ by any pairwise error probability $P(0 \to c)$ and show that $d \leq 2$ in a similar way as in (9)&(10). ■

Let $(x_1, x_2, \ldots, x_N) = (x_1^{N/2}, x_{N/2+1}^N)$ be a codeword. A block-erasure channel (block-BEC) is defined as follows: The codeword is divided into $B=2$ blocks, $x_1^{N/2}$ and $x_{N/2+1}^N$. The two blocks are independently erased by the channel. Let the symbol '?' represent an unknown value (scalar or vector), then the rigorous definition of the block-erasure channel becomes:

*Definition 2:* For $0 \leq \epsilon \leq 1$, the $B=2$ block-erasure channel is a memoryless vector channel defined by the following transition probabilities:

$$P(?|x_1^{N/2}) = P(?|x_{N/2+1}^N) = \epsilon.$$

$$P(x_1^{N/2}|x_1^{N/2}) = P(x_{N/2+1}^N|x_{N/2+1}^N) = 1-\epsilon.$$

From the above definition and the first equality in (3), we deduce that a message $\Lambda$ can take two possible values on a block-erasure channel. If a block is erased, then all its symbols have a channel message $\Lambda = 0$. If a block is not erased (perfectly copied at the channel output), then all its symbols have a channel message $\Lambda = +\infty$. Also, for the block-BEC, full diversity is equivalent to $P_e = \epsilon^2$ [9], i.e. the definition of diversity is $d = \lim_{\epsilon \to 0} \frac{\log(P_e)}{\log(\epsilon)}$.

*Proposition 1:* For a linear binary code $\mathcal{C}[N,K]$, under maximum-likelihood decoding, full diversity on the block-erasure channel is equivalent to full diversity on the block-fading channel.

*Proof:* Necessary condition: Assume that $\mathcal{C}[N,K]$ is FD on the block-fading channel. Then, from Lemma (1) we have $\omega_1(c) \neq 0$ and $\omega_2(c) \neq 0$ for all non-zero codewords. If $x_{N/2+1}^N$ is erased with probability $\epsilon$, the decoder can distinguish between $0$ and $c$ thanks to $x_1^{N/2}$. The latter is non-zero and no other codeword has an identical $x_1^{N/2}$ otherwise $\omega_1 = 0$ by linearity. Thus, the ML decoder makes an error on the block-BEC if and only if the two blocks are erased, i.e. $P_e = \epsilon^2$.

Sufficient condition: Assume that $\mathcal{C}[N,K]$ is FD on the block-erasure channel. A similar reasoning leads to $\omega_1(c) \neq 0$ and $\omega_2(c) \neq 0$ which is FD on the block-fading channel. ■

Proving FD-equivalence between the block-BEC and the block-fading channel under ML decoding of a linear binary code seems quite simple as shown above. Does this property hold under iterative decoding of LDPC codes? Let us analyze the channel behavior via the fading plane approach [10]. We will prove FD-equivalence for any code equipped with any decoding algorithm. The equivalence between fading and erasure is intrinsic to the channel.

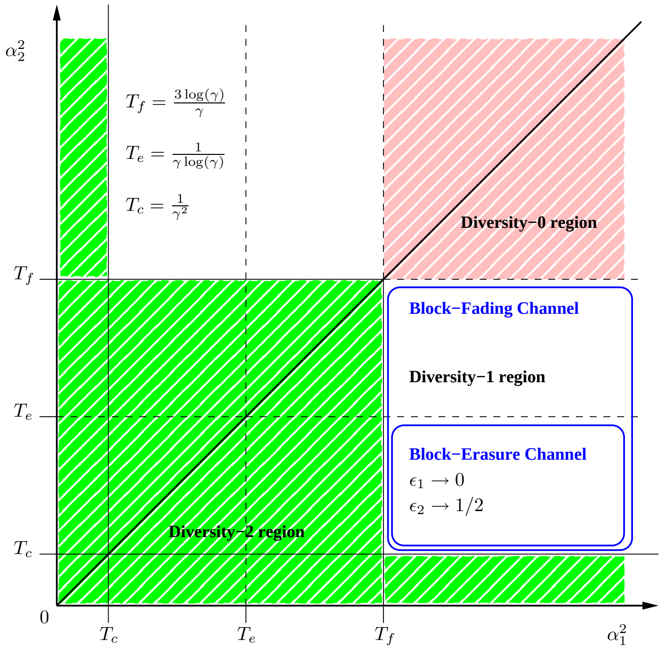


Fig. 1. Fading plane showing the different diversity regions for the analysis of coding on the block-fading channel.

Consider the top-right quarter of the bidimensional place where $\alpha_1^2$ represents the abscissa and $\alpha_2^2$ represents the ordinate. The channel is symmetric and we assume that $\mathcal{C}[N,K]$ is an LDPC code symmetric with respect to $\alpha_1$ and $\alpha_2$, i.e. the LDPC ensemble has an identical graph structure for both half-codewords $x_1^{N/2}$ and $x_{N/2+1}^{N}$. Hence, it is sufficient to make the analysis for $\alpha_2^2 \leq \alpha_1^2$. The fading plane is partitioned into regions as illustrated in Fig.1. Three thresholds on the value of the squared fading are required, in increasing order they are $T_c$, $T_e$, and $T_f$. These thresholds will delimit regions at different diversity orders. Firstly, let us recall that if $P_e = K/\gamma^d$, then $-\lim_{\gamma\rightarrow+\infty}\frac{\log(P_e)}{\log(\gamma)} = d$ iff $\log(K) = o(\log(\gamma))$, i.e. $K$ can vary with the signal-to-noise ratio but $\log(\gamma)$ must dominate $\log(K)$ in order to yield a diversity equal to $d$. Any $K$ in the form $K = (\log(\gamma))^j$, $j \in \mathbb{Z}$ or $K = j\log(\gamma)$, $j \in \mathcal{N}$, is suitable for satisfying the property $\log(K) = o(\log(\gamma))$.

We start by determining the limits of the diversity-2 region. If both $\alpha_1^2$ and $\alpha_2^2$ are less than $T_f = \frac{3\log(\gamma)}{\gamma}$ (the choice of the numerator for this full-diversity threshold will be justified below), then

$$P(\alpha_1^2 \leq T_f, \alpha_2^2 \leq T_f) \approx \frac{(3\log(\gamma))^2}{\gamma^2} \doteq \frac{1}{\gamma^2},$$

for $\gamma \gg 1$, where $\doteq$ means that both sides have the same diversity order. To get the whole diversity-2 region, we need to add the area under $\alpha_2^2 \leq T_c$ for $\alpha_1^2 \geq T_f$ and the symmetric part along the ordinate axis. Indeed,

$$P(\alpha_1^2 \geq T_f, \alpha_2^2 \leq T_c) \approx (1-\frac{3\log(\gamma)}{\gamma})\frac{1}{\gamma^2} \doteq \frac{1}{\gamma^2},$$

for $\gamma \gg 1$. The additional area defined by $T_c = \frac{1}{\gamma^2}$ (referred to as the capacity threshold) corresponds to the case where a unique fading event has probability less than $\frac{1}{\gamma^2}$. The strip under $T_c$ includes the rate-$1/2$ binary-input capacity outage boundary [10] for a 2-state block-fading Rayleigh channel. The diversity-1 region is defined by $\alpha_2^2$ in the range $[T_c, T_f]$ and $\alpha_1^2$ greater than $T_f$,

$$P(\alpha_1^2 \geq T_f, T_c \leq \alpha_2^2 \leq T_f) \doteq \frac{1}{\gamma}.$$

The diversity-0 region is determined by taking both squared fadings greater than $T_f$,

$$P(\alpha_1^2 \geq T_f, \alpha_2^2 \geq T_f) \doteq 1.$$

Finally, the choice of $T_e = \frac{1}{\gamma\log(\gamma)}$ (the erasure channel threshold) will be justified below.

What is the effect of block fading on the code performance under a given decoding algorithm? Let $\epsilon_1 = Q(\sqrt{2\alpha_1^2\gamma})$ and $\epsilon_2 = Q(\sqrt{2\alpha_2^2\gamma})$ be the uncoded error probabilities on the block-fading channel.

• **The diversity-0 region:** $\alpha_1^2 \geq T_f = 3\log(\gamma)/\gamma$, using the upper bound $Q(x) \leq \exp(-x^2/2)$, we get $\epsilon_1 \leq 1/\gamma^3$. Similarly we have $\epsilon_2 \leq 1/\gamma^3$. Even without decoding, a symbol-by-symbol hard decision at the channel output provides $P_e \doteq \frac{1}{\gamma^3}$ in this region! This diversity order of 3 for $P_e$ is due to the factor 3 in $T_f$. A factor of 2 would have been sufficient to study the FD-equivalence, but we wanted to emphasize that the diversity-0 region has no relevance while building a root-LDPC code.

• **The diversity-2 region:** In this region, a failure of the decoder, for any type of decoding algorithm, would generate a diversity order of 2 which is the probability of the point $(\alpha_1^2, \alpha_2^2)$ to belong to this region. Thus, from diversity order point of view, the diversity-2 region has no influence on the performance of a root-LDPC code. From coding gain point of view, see (14), the decoding threshold should be optimized on different points in the fading plane in order to approach the capacity outage boundary. The root-LDPC code design in [1][2] took into account two areas in the fading plane, the ergodic line and the very unbalanced regime. In [12], an optimization in the fading plane has been made for random LDPC ensembles at rate slightly less than $1/2$.

• **The diversity-1 region:** This is the most critical region in the fading plane. As shown above, the diversity-0 and the diversity-2 regions have no influence on the diversity order of an error-correcting code. On the contrary, a decoder that fails in the diversity-1 region would yield an error probability $P_e \doteq \frac{1}{\gamma}$, i.e. full diversity is lost. Let us focus on the sub-area defined by $\alpha_1^2 \geq T_f$ and $\alpha_2^2$ in the range $[T_c, T_e]$. In that sub-area, for $\gamma \gg 1$, we have $\epsilon_1 \leq Q(\sqrt{6\log(\gamma)}) \rightarrow 0$ and $\epsilon_2 \geq Q(\sqrt{\frac{2}{\log(\gamma)}})$, but $\epsilon_2 \leq 1/2$, this proves that $\epsilon_2 \rightarrow 1/2$. In this extremal case, $\epsilon_1 = 0$ is equivalent to a message $\Lambda_1 = +\infty$ and $\epsilon_2 = 1/2$ is equivalent to a message $\Lambda_2 = 0$. The fading channel is behaving like a block-erasure channel in the strip $[T_c, T_e]$. The choice of the threshold $T_e$ is judicious and makes $\epsilon_2 \rightarrow 1/2$. In the proof of Proposition (3), with the addition of two decoding strategies, it is proven that the block-fading channel is identical to a block-erasure channel in the strip $[T_c, T_e]$.

In [1][2], the block-erasure channel has been considered as a special case of the block-fading channel by forcing the extremal values $\alpha_1^2 = +\infty$ and $\alpha_2^2 = 0$, which is equivalent to $\Lambda_1 = +\infty$ and $\Lambda_2 = 0$. In [11], a proof of full diversity is given for rootchecks in a product code on a block-fading channel. Another proof is given in [1] for rootchecks in a low-density parity-check code. In the sequel, we establish a new proof for FD-equivalence between the block-BEC and the block-fading channel.

*Proposition 2:* Let $\mathcal{C}$ be a binary code equipped with a given decoding algorithm. Full-diversity on the block-fading channel results in full-diversity on the block-erasure channel.

*Proof:* If full diversity is achieved by the decoder, then it is achieved in the diversity-1 region. Therefore, full diversity is also achieved in the strip $[T_c, T_e]$ where the channel has block erasures. In a formal way, let us denote the diversity-$i$ region by $\mathcal{R}_i$, i=0,1,2. We get

$$P_e = \sum_{i=0}^{2} E_{\mathcal{R}_i}[P_e(\alpha_1, \alpha_2)], \tag{11}$$

where $P_e(\alpha_1, \alpha_2)$ is the conditional error probability and $E_{\mathcal{R}_i}[]$ denotes mathematical expectation with respect to the fading distribution made over the region $\mathcal{R}_i$. For $i = 0$ and $T_f = \frac{3\log(\gamma)}{\gamma}$, we have

$$E_{\mathcal{R}_0}[P_e(\alpha_1, \alpha_2)] \ \leq \ E_{\mathcal{R}_0}[1] P_e^{max}(\mathcal{R}_0) \ \dot{\leq} \ \frac{1}{\gamma^3}.$$

where $P_e^{max}(\mathcal{R}_0)$ is the maximum of the conditonal error proabability in the region $\mathcal{R}_0$. Similarly, for $i = 2$ and the judicious choice of $T_c$ and $T_f$,

$$E_{\mathcal{R}_2}[P_e(\alpha_1, \alpha_2)] \ \leq \ E_{\mathcal{R}_2}[1] \doteq \frac{1}{\gamma^2}.$$

Thirdly, for $i = 1$,

$$E_{\mathcal{R}_1}[P_e(\alpha_1, \alpha_2)] \ \leq \ E_{\mathcal{R}_1}[1] P_e^{max}(\mathcal{R}_1) \ \doteq \ \frac{1}{\gamma} P_e^{max}(\mathcal{R}_1),$$

Finally, we obtain

$$P_e \ \dot{\leq} \ \frac{1}{\gamma^3} + \frac{1}{\gamma^2} + \frac{1}{\gamma} P_e^{max}(\mathcal{R}_1),$$

which becomes

$$P_e \ \dot{\leq} \ \frac{1}{\gamma^2} + \frac{1}{\gamma} P_e^{max}(\mathcal{R}_1) \tag{12}$$

Let $\mathcal{S} \subset \mathcal{R}_1$ denote the block-erasure strip defined by $\alpha_1^2 \geq T_f$ and $\alpha_2^2 \in [T_c, T_e]$. If the decoder is FD on the block-fading channel, from (12) we find $P_e^{max}(\mathcal{R}_1) \dot{\leq} \frac{1}{\gamma}$. But $P_e^{max}(\mathcal{S}) \leq P_e^{max}(\mathcal{R}_1)$, then the decoder is also full-diversity on the block-erasure channel. ■

*Proposition 3:* Let $\mathcal{C}$ be a binary code equipped with a given decoding algorithm. Full diversity on the block-erasure channel results in full-diversity on the block-fading channel.

*Proof:* Notations from the proof of the previous propositions are used. In the strip $\mathcal{S}$ inside the region $\mathcal{R}_1$, we saw that $\epsilon_1 \rightarrow 0$ and $\epsilon_2 \rightarrow 1/2$. More precisely, in the strip $\mathcal{S}$, from $T_f \leq \alpha_1^2$ and $\alpha_2^2 \leq T_e$ we have at large $\gamma$

$$\epsilon_1 = Q(\sqrt{2\alpha_1^2 \gamma}) \ \leq \ \frac{1}{\gamma^3},$$

$$\frac{1}{2} - \epsilon_2 = \frac{1}{2} - Q(\sqrt{2\alpha_2^2 \gamma}) \leq \frac{1}{\sqrt{\pi \log(\gamma)}} + o(\frac{1}{\sqrt{\log(\gamma)}}).$$

$\epsilon_2$ is approaching $1/2$ at a speed $\frac{1}{\sqrt{\log(\gamma)}}$. Then, we adopt the following decoding strategy regarding $\alpha_2^2$ in $\mathcal{S}$: *The decoder decides to force all messages to* $\Lambda_2 = 0$, *i.e. it declares an erasure on all bits transmitted on the second fading*. Similarly, $\epsilon_1$ is vanishing at a speed with diversity order equal to 3. Hence, every bit transmitted on the first fading is correct ($\Lambda_1 = +\infty$) with probability greater than $1 - \frac{1}{\gamma^3}$ and it is incorrect with probability less than $\frac{1}{\gamma^3}$. Then, we adopt the following decoding strategy regarding $\alpha_1^2$: *The decoder decides to force all messages to* $\Lambda_1 = +\infty$, *i.e. all bits transmitted on the first fading are assumed to be correctly received*. This strategy would only add an extra error probability vanishing as $\frac{1}{\gamma^3}$ which has no effect on the FD property because $\frac{1}{\gamma^3} + \frac{1}{\gamma^2} \ \doteq \ \frac{1}{\gamma^2}$.

Under the two strategies described above, the block-fading channel is identical to a block-erasure channel in the strip region $\mathcal{S}$ defined by $\alpha_1^2 \geq T_f$ and $\alpha_2^2 \in [T_c, T_e]$.

Now, consider a fading point $(\alpha_1^2, \alpha_2^2)$ located above $\mathcal{S}$ as shown in Fig. 2 We adopt the following decoding strategy in the diversity-1 region:
*If* $\alpha_2^2 > T_e$ *then force its value to* $\alpha_2^2 = T_e$, *i.e. make a projection of the fading point onto the strip* $\mathcal{S}$. The projection does not need to be orthogonal! Any projection preserving $\alpha_1^2 \geq T_f$ is valid. Under this third strategy, the block-fading channel in the region $\mathcal{R}_1$ is converted into a block-erasure channel in the strip $\mathcal{S}$. Therefore, if the decoder is FD on the block-BEC, it is also FD on the block-fading channel. ■

*Corollary 1:* Under all types of decoders (ML, BP or Min-Sum), for any LDPC code, full diversity on the block-fading channel is equivalent to full diversity on the block-erasure channel.

*Proof:* The full-diversity equivalence statement results from combining the two previous propositions. This corollary is also valid for non-LDPC codes such as Turbo codes [8], Product Codes [11], etc. Indeed, the proofs of Propositions 2 & 3 rely on intrinsic channel properties and nothing is related to the code structure. It's generalization to $B$ fadings, $B > 2$, should be straightforward. ■

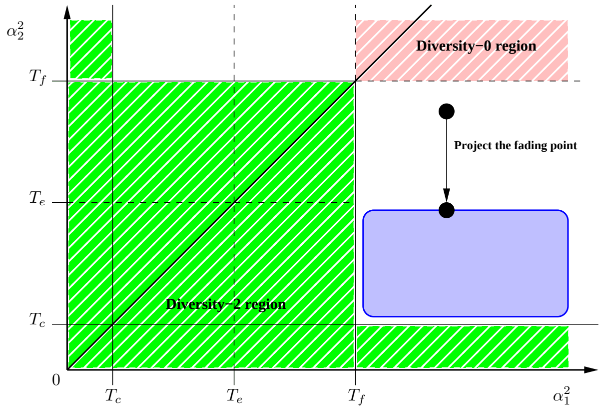


Fig. 2. Making a projection of the fading point onto the strip $\mathcal{S}$. This allows to extend full diversity from a block-erasure to a block-fading channel.

*Corollary 2:* For any LDPC code on a block-fading channel, full diversity under BP decoding results in full diversity under Min-Sum decoding. In other words, the sub-optimal decoder does not induce a loss in diversity!

*Proof:* The proof is based on the FD-equivalence property stated in Corollary 1 and applied to both BP and Min-Sum. If the BP decoder is FD on the block-fading channel, then it is FD on the block-erasure channel. But BP and Min-Sum are identical on the block-erasure channel (the two algorithms collapse into a unique algorithm). Now we have FD for Min-Sum on the block-erasure channel which results in FD for Min-Sum on the block-fading channel. ∎

Root-LDPC codes proposed in [1] include special checknodes referred to as rootchecks. A rootcheck is depicted in Fig. 3. The $N$-length $1/2$-rate root-LDPC contains $N/2$ rootchecks, one for each information bit. If the bit at the root is erased, it is immediately solved from the rootcheck leaves in one decoding iteration. Using FD-equivalence of Corollary 1, it is proven that a root-LDPC code attains full diversity on a block-fading channel.

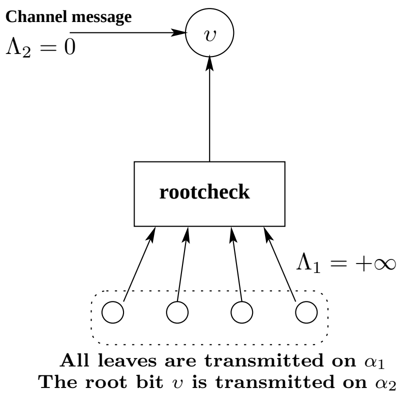


Fig. 3. Rootcheck for an information bit in a root-LDPC code. Other checknodes connected to the information bit $\upsilon$ are not shown in this illustration.

When all information bits are solved[1] after one decoding iteration, parity bits in root-LDPC codes observe a diversity evolution via uncontrolled rootchecks. This phenomenon is described in the next section and it is shown how this can further help information bits.

## III. Diversity Population Evolution

Information bits are divided into classes $1i$ and $2i$. Similarly, parity bits are grouped into two classes $1p$ and $2p$. The transmission order on the block-fading channel follows the channel definition in (1)&(2). Double diversity for $1i$ is guaranteed by rootchecks whose leaves are only connected to $2i$ and $2p$. The matrix description is depicted in Fig. 4. Class $1i$ is connected to rootchecks $1c$ via an identity matrix (or any permutation matrix in general). Class $1i$ is also connected to $2c$ via a $N/4 \times N/4$ random sparse matrix $H_{1i}$. Class $1p$ has no edges to checknodes $1c$, only to checknodes $2c$ via a $N/4 \times N/4$ random sparse matrix $H_{1p}$. The structure is symmetric and two other sparse random matrices $H_{2i}$ and $H_{2p}$ define edges linked to bits $2i$ and $2p$.

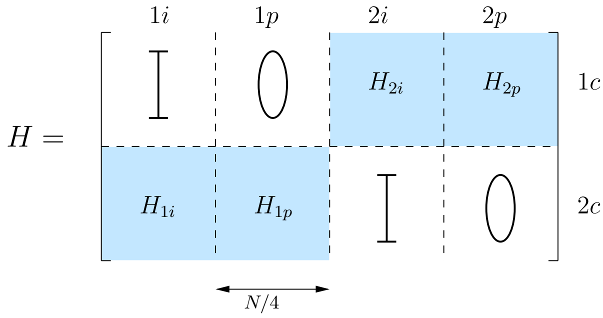


Fig. 4. The parity-check matrix for a $1/2$-rate root-LDPC, it shows 4 classes of bits and 2 classes of checks.

Now we distinguish two ensembles [2] of root-LDPC codes (other ensembles will be defined later in this paper).

- **Root-LDPC($2\pi$) ensemble:** A unique set of edges is generated for the $N/4 \times N/2$ submatrix $[H_{1i}|H_{1p}]$ and another set of edges is generated for the $N/4 \times N/2$ submatrix $[H_{2i}|H_{2p}]$. This ensemble is defined by two edge permutations ($2\pi$). In the sequel, this ensemble will be referred to as **Root-LDPC-I**.
- **Root-LDPC($4\pi$) ensemble:** Four different set of edges are generated for the four submatrices $H_{1i}$, $H_{1p}$, $H_{2i}$, and $H_{2p}$ respectively. This ensemble is defined by four edge permutations ($4\pi$). In the next section, 4 ensembles derived from Root-LDPC($4\pi$) will be defined.

The absence of rootchecks for parity bits does not necessarily lead to incomplete diversity. For example, full-diversity product codes [11] always show full diversity on both information and parity bits. The proof that any FD product code must solve all its bits after 3 decoding iterations is based on high-order

[1] This is an abuse of terminology. Instead of saying 'full' or 'double diversity', we may say that the binary element has been solved. It is permitted because of the erasure-fading FD-equivalence.

rootchecks [11]. An illustration of a second-order rootcheck is given in Fig.5. One or more leaf-bits are connected to a first-order rootcheck. After two decoding iterations the bit at the top of the second-order rootcheck is solved. The random structure of the root-LDPC matrix may create such high-order rootchecks, a phenomenon named *uncontrolled diversity doping* for parity bits or equivalently *diversity population evolution* (DPE). The DPE behavior depends on the two subgraphs defined by the submatrices $H_{1p}$ and $H_{2p}$.

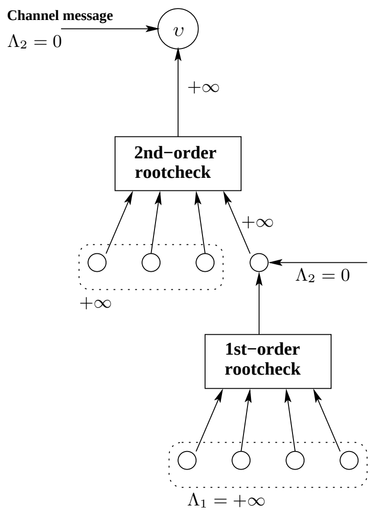


Fig. 5. A second-order rootcheck for an information bit or a parity bit in a root-LDPC code. Two decoding iterations are needed to achieve full diversity.

Let $p_m$ be the fraction of parity bits attaining full diversity at iteration $m$ in a root-LDPC-I ensemble. Suppose that the degree distribution of the root-LDPC-I is defined by the polynomials $\lambda(x)$ and $\rho(x)$ from an edge perspective for bitnodes and checknodes respectively. It has been shown in [2] that

$$p_{m+1} = 1 - \lambda(1 - \tilde{\rho}(f_e + (1 - f_e)p_m)), \qquad (13)$$

where $\tilde{\rho}(x)$ is the new distribution obtained by deleting one edge from every checknode, the multiedge fraction is $f_e = \frac{\bar{d}_b - 1}{2\bar{d}_b - 1}$, and $\bar{d}_b$ is the average bitnode degree. Expression (13) show how the population of FD parity bits evolves with decoding iterations. At $m = 0$ we have $p_0 = 0$ since all parity bits are erased, then $p_\infty$ is determined as the first fixed point at the right from the origin.

How $p_\infty$, the final fraction of full-diversity parity bits, can influence the performance of the root-LDPC ensemble?

First answer (trivial): On vector channels and channels with interference (MIMO [13], CDMA [14], and ISI channels [15]) improving the performance of parity bits should boost the *a priori* information (known as extrinsic information) delivered to the interference cancellation detector.

Second answer (less trivial): Diversity population evolution results in coding gain evolution (CGE), the key idea is in the main difference between the block-erasure channel and the block-fading channel.

On a block-erasure channel, if a binary element is solved by one checknode, there is no need to solve it again via another checknode. In other words, using (3) and (4), if a bit $2i$ is erased by the channel because $\Lambda_2 = \alpha_2^2 = 0$, its rootcheck will deliver a message including $\Lambda_1 = \alpha_1^2 = \infty$. The final message would have the form $\Lambda = \xi\alpha_1^2 + \zeta\alpha_2^2$. But since $\alpha_1^2 = \infty$, the energy coefficient $\xi$ has no effect on the block-erasure channel. Coding gain does not exist on a block-erasure channel. Indeed, a code achieving full diversity on block-BEC will also attain the outage limit [9].

On a block-fading channel, the total performance depends on the diversity order and the so-called coding gain. At large signal-to-noise ratio, we have [3]

$$P_e \approx \frac{K}{\gamma^d} = \frac{1}{(g \cdot \gamma)^d}, \qquad (14)$$

where $g$ is the coding gain. There is no analytical method to determine $g$ for a given root-LDPC instance or for a given root-LDPC ensemble! The coding gain $g$ depends on the energy coefficients $\xi$ and $\zeta$. Increasing $\xi$ should also increase $g$. If a bit $2i$ is badly received because $\alpha_2^2 < T_f$, its rootcheck will deliver a high-confidence message based on $\alpha_1^2 > T_f$. The general form $\Lambda = \xi\alpha_1^2 + \zeta\alpha_2^2 + \eta$ shows us that immunity against additive noise $\eta$ is reinforced by doping the energy coefficient $\xi$. If another checknode is capable of delivering a high-confidence message (i.e. solve the same bit twice) this would increment $\xi$ by 1. If a bitnode has degree $d_b$, the maximum value for $\xi$ is $d_b - 1$, it corresponds to the case where all neighboring checknodes are solving the bitnode. As a conclusion, it is beneficial to solve a bit many time via different checknodes on a block-fading channel.

Let $v$ be a bitnode from class $1i$. Assume that $v$ is connected to one rootcheck $\Psi_1$ from class $1c$ and to another checknode $\Psi_2$ from the class $2c$. The checknode $\Psi_2$ includes parity bits from class $1p$ as leaves. Thanks to DPE, it is possible to solve those parity bits, then the checknode $\Psi_2$ will solve $v$ again, i.e. $\xi = 2$. The checknode $\Psi_2$ is a high-order rootcheck for $v$. Diversity on parity bits generates a gain doping for information bits. In other words CGE is linked to DPE via $p_\infty$.

Consider the root-LDPC-I ensemble defined by its degree distribution $\lambda(x)$ and $\rho(x)$. Assume that the channel is block-BEC then apply density evolution [4][5] on the graph structure. Modify the density evolution algorithm by saving the number of times a bit is solved, i.e. save and propagate the value of $\xi$. The obtained algorithm is a CGE algorithm [2]. It is a numerical method for finding how $\xi$ evolves with iterations. In the steady state, after an infinite number of decoding iterations, it is possible to find a lower bound for $\xi$. We know that a fraction $p_\infty$ of parity bits is solved. We assume that every checknode connected to an information bit delivers '+1' as energy coefficient each time all its leaf-bits are solved. This is a lower bound because the contribution of 3rd-order rootchecks and beyond is not counted for. The lower bound on the total energy coefficient has PMF [2]

$$F_\infty(\xi = n+1) = \frac{1}{n!}\left(\frac{\pi_e}{1-\pi_e}\right)^n \left[x^n \frac{\partial^n \tilde{\lambda}(x)}{\partial x^n}\right]_{x=(1-\pi_e)}$$

where $1 \leq \xi \leq d_b - 1$ and $\pi_e = \tilde{\rho}\left(f_e + (1-f_e)p_\infty\right)$.
From the above expression, we can find the PMF of $\xi$ given $\lambda(x)$ and $\rho(x)$. This doping is uncontrolled and determining the optimal degree distribution in terms of $p_\infty$ and $\xi$ is out of the scope of this paper. In general, the PMF of $\xi$ improves with $p_\infty$ (it is not monotonic because of the influence of $\lambda(x)$ and $\rho(x)$). As suggested in [2], we will force parity bits to be solved after some number of decoding iterations by embedding extra high-order rootchecks in the code structure. This controlled doping is described in the next section.

## IV. CONTROLLED DOPING IN ROOT-LDPC CODES

In this section, only quasi-regular root-LDPC codes are considered. We propose new ensembles of root-LDPC codes by modifying the original (3,6)-regular root-LDPC-I ensemble. The purpose of controlled and uncontrolled doping is to improve the energy coefficient of information bits after solving parity bits. Hence, a parity bit is firstly solved from a set of information bits and other previously solved parity bits. Then, the parity bit should transmit a high-confidence message to a new information bit. Uncontrolled doping recorded in [2] corresponds to a DPE steady-state parameter $p_\infty = 7.82\%$ for a (3,6)-regular root-LDPC. The best fraction $p_\infty$ of full-diversity parity bits recorded in [2] was about $17\%$ for some irregular root-LDPC-I ensembles.

Controlled doping can achieve a fraction $p_\infty$ as high as $100\%$. The matrix given in Fig.4 is modified by introducing a smaller identity (or a permutation) matrix for parity bits. Fig. 6 shows the matrix for a root-LDPC code with $50\%$ of controlled doping.

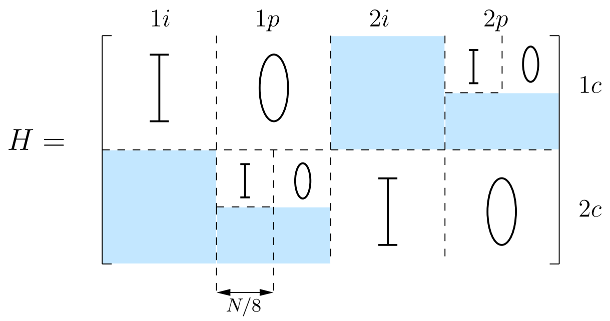


Fig. 6. Root-LDPC with controlled doping. Half of the parity bits are forced to full diversity after 2 decoding iterations.

The submatrix $H_{1p}$ has the following form

$$H_{1p} = \left[\begin{array}{cc} \mathrm{I} & \mathrm{O} \\ \multicolumn{2}{c}{H_{pp}} \end{array}\right], \tag{15}$$

where $I$ is an identity/permutation matrix, **O** is the $N/4 \times N/4$ zero matrix, and $H_{pp}$ is a $N/8 \times N/4$ random sparse matrix. When $1i$ and $1p$ are erased, $\alpha_1 = 0$ and $\alpha_2 = \infty$, $1i$ is determined after one iteration via the top left identity in $H$, then at the second iteration the first $N/8$ bits $1p$ are determined via the top left matrix in $H_{1p}$.

Before defining new ensembles, let us freeze the choice of submatrices $H_{1i}$ and $H_{2i}$ (defined in Fig.4). It is supposed that $H_{1i}$ and $H_{2i}$ belong to the set of $N/4 \times N/4$ random binary matrices with Hamming weight equal to 3 per row (so is the weight per column). We will use the notation

$$H_{1i} = H_{1i}(\updownarrow 3, \overleftrightarrow{3}).$$

Four independent edge permutations are needed to construct $H_{1i}$, $H_{2i}$, $H_{pp}$ in $H_{1p}$, and $H_{pp}$ in $H_{2p}$. Thus, the ensemble defined by $H$ as in Fig.6 is a root-LDPC($4\pi$) ensemble[2].

*Definition 3:* The ensemble root-LDPC-II is a root-LDPC($4\pi$) ensemble with $H_{1p}$ defined by (15) and

$$H_{pp} = H_{pp}(\updownarrow 1.5, \overleftrightarrow{3}).$$

Since we are studying quasi-regular codes, $H_{pp}$ in root-LDPC-II has a weight of 3 per row. Half of its columns have weight 1 and the others have weight 2 (average is 1.5). For the whole matrix structure $H$, we have $\bar{d}_b = 3$ and $\bar{d}_c = 6$.

*Proposition 4:* Uncontrolled doping of parity bits in the ensemble root-LDPC-II admits $p_\infty = 2 - \sqrt{3} = 26.8\%$.

*Proof:* The proof is very similar to the one for (13). It is mainly based on the erasure channel approach. In $H_{pp}$, the local bitnode distribution from a node perspective is $\mathring{\lambda}(x) = \frac{1}{2} + \frac{1}{2}x$. Thus, from edge perspective we have $\lambda(x) = \frac{1}{3} + \frac{2}{3}x$. The row distribution is $\rho(x) = x^2$. At iteration 0, 50% only of parity bits are erased (thanks to 50% of controlled doping). So we have $p_0 = \frac{1}{2}$. Then, evolution in the tree graph of the ensemble yields

$$\frac{(1-p_{m+1})}{2} = \frac{1}{2} \cdot \lambda(1 - \rho(1 - \frac{(1-p_{m+1})}{2})).$$

Finally, $p_\infty$ is solution of the polynomial $x^2 - 4x + 1$. The valid root is $p_\infty = 2 - \sqrt{3} = 26.8\%$. ■

From proposition (4), we find that $50 + \frac{1}{2}26.8 = 63.4\%$ is the total fraction of full diversity parity bits for root-LDPC-II. That fraction is $7.82\%$ for the original (3,6)-regular root-LDPC-I. In the new ensemble, uncontrolled doping (13.4%) is dominated by controlled doping (50%). Now, for finite length $N$, we would like to experimentally find the performance of a code chosen from the root-LDPC-II ensemble. Decoding is made via a standard BP. Apparently, there should be no weakness in the ensemble for finite $N$.

*Definition 4:* For finite length, a root-LDPC code is said to be *FD-Encodable* if $1p$ and $2p$ parity bits can be uniquely

[2]This is a relaxed root-LDPC($4\pi$) when compared to the one defined in [2]. Here, it is possible to have a different $\lambda(x)$ polynomial for $1i$ and $1p$. Also, there is no restriction on the minimal checknode degree. The relaxed ensemble has a non-zero $p_\infty$.

determined from $1i$ and $2i$ information bits, while maintaining full diversity for information bits.
It is obvious that a code is FD-Encodable iff $H_{1p}$ and $H_{2p}$ are both full-rank binary matrices. In the ensemble root-LDPC-II, the following patterns appear in the rows of $H_{pp}$: All ones at one side of $H_{pp}$, $111|000$ and $000|111$, occuring with probability $1/8$. Two ones at one side of $H_{pp}$, $110|100$ and $100|110$, occuring with probability $3/8$. Unfortunately, for large $N$, the right $N/8 \times N/8$ part of $H_{pp}$ would include $N/64$ zero rows on average. Consequently, $H_{1p}$ is not full-rank and its rank is diminished by at least $N/64$ for $N \gg 1$. Codes in the root-LDPC-II ensemble are not FD-Encodable!

This rank deficiency issue may also occur in other root-LDPC ensembles [16] involved with doping, when the graph code is designed to bring diversity to its parity bits and then to bring back coding gain for its information bits. The authors in [16] discovered this weakness when attempting to encode an instance from a root-LDPC ensemble, where high-confidence messages have been forced back from FD parity bits to information bits. In some general root-LDPC ensemble, let us make a simple observation on $H_{1p}$ when a fraction $p_\infty$ of bits is well known

$$H_{1p} = \left[ \begin{array}{cc} A & \mathrm{O} \\ \multicolumn{2}{c}{H_{pp}} \end{array} \right] = \left[ \begin{array}{cc} A & \mathrm{O} \\ B & C \end{array} \right], \qquad (16)$$

where $A$ is $(p_\infty N)/4 \times (p_\infty N)/4$. The submatrix $A$ has full rank because the corresponding parity bits have been solved from information bits, by controlled or uncontrolled doping. If $A$ has a special structure such that high-confidence messages are going back to information bits from its proper checknodes, then it is possible to select a full-rank submatrix $C$ to make the code FD-Encodable. Unfortunately, if doping checknodes have been created by forcing to zero some rows in $C$ then the code is no more FD-Encodable. It results in the obligation of permuting parity bits with information bits. Thus, $1p$ bits becoming information bits do not necessarily guarantee a full-diversity code. Two types of solutions are given below to overcome the rank deficiency problem.

*Proposition 5:* A code instance chosen in the Root-LDPC-II ensemble becomes FD-encodable via the application of a permutation-restricted Gaussian elimination and code shortening. The new coding rate $R$ satisfies $R \leq \frac{15}{31}$.

*Proof:* Encoding is made by writing $H$ in its systematic form (we are not taking into account fast encoding methods). Hence, a Gaussian elimination procedure is applied on $H$ to create an $N/2 \times N/2$ identity instead of the submatrix containing $H_{1p}$ and $H_{2p}$. While processing a column within $H_{1p}$, each time a 1 is not found on that column under the diagonal, the procedure is forced to switch with a valid column from the set covering $2i$ bits. Similarly, while processing $H_{2p}$, if 1 is not found in a column under the diagonal, we switch the current column with another valid column in the sets covering $1i$ bits. This permutation-restricted Gaussian elimination will never fail because information bits are covered by two identity matrices facing both $H_{1p}$ and $H_{2p}$.
After terminating the Gaussian elimination algorithm, all previous parity bits switched to information bits positions will be forced to zero in order to maintain full diversity (this is shortening). If $L_1$,$L_2$ column permutations occurred in $H_{1p}$ and $H_{2p}$ respectively, then the new rate becomes ($L = L_1 + L_2$):

$$R = \frac{K-L}{N-L} \ \leq \ \frac{N/2 - N/32}{N - N/32} = \frac{15}{31},$$

from $K = N/2$ and $L = L_1 + L_2 \geq 2 \cdot N/64$, for large $N$. ■

We would like to force doping in a root-LDPC without rate loss due to rank deficiency. Let us define a new ensemble referred to as root-LDPC-III.

*Definition 5:* The ensemble root-LDPC-III is a root-LDPC($6\pi$) ensemble with $H_{1p}$ defined by (15) and

$$H_{pp} = [\ B \mid C\ ],$$

where

$$B = B(\updownarrow 1, \overleftrightarrow{1}) \quad \text{and} \quad C = C(\updownarrow 2, \overleftrightarrow{2}).$$

A $C(\updownarrow 2, \overleftrightarrow{2})$ binary matrix is always rank deficient (just add all rows). Thus, $C$ is slightly modified by making one column of unit weight and one row of unit weight. The edge permutation defining $C$ is generated such that $C$ has full rank. Therefore, it is always possible to build an FD-Encodable instance from the rate-1/2 root-LDPC-III ensemble. As a convention, we will keep the notation $C(\updownarrow 2, \overleftrightarrow{2})$ even if one row has a unit weight and one column has a unit weight. For the whole matrix structure $H$, this ensemble also has average bitnode degree $\bar{d}_b = 3$ and average checknode degree $\bar{d}_c = 6$.

The root-LDPC-III ensemble embeds 50% of controlled doping. The top left part of $H_{1p}$ is forcing 50% of parity bits to full diversity after two decoding iterations. At this point, we would like to establish a result similar to Proposition (4). Before establishing such an intriguing statement, let us take a deeper look at $C(\updownarrow 2, \overleftrightarrow{2})$.

*Proposition 6:* Let $C(\updownarrow 2, \overleftrightarrow{2})$ be a full rank $N/8 \times N/8$ matrix. Then, the bipartite graph defined by $C$ is isomorphic to a simple chain, i.e. $C$ can be written as a double diagonal after row and column permutations.

*Proof:* The subgraph defined by $C$ has $N/8$ bitnodes and $N/8$ checknodes. All vertices have degree equal to 2 except for one bitnode and one checknode. If the subgraph contains a cycle, then the rows of $C$ associated to checknodes of that cycle will sum to zero and $C$ cannot be full-rank. Thus, the subgraph has no cycles. Consequently, it is isomorphic to a simple chain as depicted in Fig.7. ■
The chain acts like a 2-state machine (an accumulator), it can be properly terminated by transmitting a copy of the last bit. The termination of the two chains in the root-LDPC-III would

have a negligible cost in coding rate, e.g., $R = 0.499$ instead of $R = 1/2$ for code length $N = 2048$.

$$C(\updownarrow 2, \overleftrightarrow{2}) \cong \begin{bmatrix} \mathbf{1} & & & & \\ \mathbf{1} & \mathbf{1} & & & \\ & \mathbf{1} & \mathbf{1} & & \\ & & \mathbf{1} & \mathbf{1} & \\ & & & \mathbf{1} & \mathbf{1} \end{bmatrix}$$

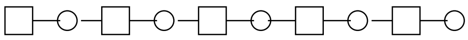

Fig. 7. The weight-2 full-rank binary random matrix $C$ is equivalent to a simple chain. This is an example with 5 vertices from each type.

*Proposition 7:* Consider an FD-Encodable instance of the root-LDPC-III ensemble. Then $p_\infty = 1 = 100\%$, i.e. all parity bits attain full diversity after a sufficient number of decoding iterations.

*Proof:* For a given checknode in the chain, the first bit is solved by the left graph and the second bit is solved by the right graph. In BCJR terminology [17], the forward processing is solving the first bit and the backward processing is solving the second bit. Hence, all bits in the chain achieve full diversity. The combination of the identity matrix in the top left part of $H_{1p}$ and the chain in the bottom right part of $H_{1p}$ yields a 100% doping for parity bits. ■

From the proof given above, we see that the two bits in a checknode are solved by the antecessor subchain and the posterior subchain respectively, not by the checknode itself. Then any checknode in the chain will send back a high-confidence message to information bits. The root-LDPC-III is capable of enhancing the energy coefficients of information bits without rank deficiency.

Other interesting ensembles can also be constructed. For example, the chain can be extended to cover the entire matrix $H_{1p}$. The root-LDPC-IV ensemble is defined by

$$H_{1p} = H_{1p}(\updownarrow 2, \overleftrightarrow{2}),$$

i.e. $H_{1p}$ is a full chain of length $N/4$ bits. The root-LDPC-V ensemble, already indicated in [2], includes identity matrices all along its diagonal as shown in Fig.8. The three root-LDPC ensembles III, IV, and V are all exhibiting a 100% doping,i.e. all parity bits are full-diversity. It is obvious that root-LDPC-V has faster convergence than root-LDPC-IV. On the contrary, the chain memory in the root-LDPC-IV is better in terms of coding gain for information bits. Therefore, we consider the root-LDPC-III ensemble as the most suitable in terms of both decoding speed and coding gain.

Finally, it is worth to mention that the graph/matrix structure of these three root-LDPC ensembles makes it possible to build an encoding circuit based on repetitors, interleavers, multiple-input xor gates for grouping, crossing wires for mixing information bits within the two streams of parity bits, and two accumulators generating a part of parity bits or all parity bits after receiving grouped and cross-grouped input bits. These encoding circuits can be directly built from the structure of the LDPC matrix. Drawings of encoding circuits are not given in this paper. The reader is invited to sketch the encoder circuit for root-LDPC-IV (relatively simple) before making the circuit for root-LDPC-III (the drawing needs an additional complexity).

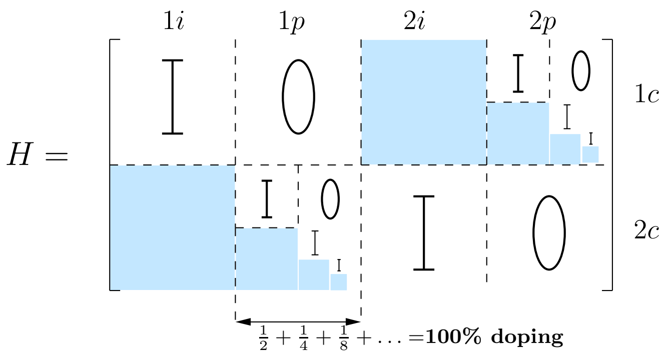


Fig. 8. Root-LDPC-V with full controlled doping. All parity bits will acquire full diversity after a large number of decoding iterations.

## V. Experimental Results

On a block-fading channel with binary input, the word error rate (WER) performance of codes from Root-LDPC-I and Root-LDPC-III ensembles are compared. As expected, the WER for parity bits behaves like $1/\gamma$ in absence of doping. For Root-LDPC-III, the WERs of information and parity bits are superimposed and decrease as $1/\gamma^2$.

The second context shows the WER for codes from ensembles root-LDPC-I & III versus a fully random ensemble. The latter is a (3,6)-regular code. The channel is quasi-static MIMO with 2 transmit antennas and two receive antennas. For this channel, we have $d_0 = 2$, $d_s = 2$, and $d = 4$. The doping of Root-LDPC-III translates into true gain. Also, as expected, the fully random ensemble cannot guarantee a full diversity $d = 4$. Transmit diversity is guaranteed for root-LDPC codes without the use of linear precoders or block space-time codes.

## VI. Conclusions and Perspectives

In this paper, we gave a new proof for the full-diversity equivalence between block-fading and block-erasure channels. Diversity Population Evolution and Doping in root-LDPC code ensembles are reviewed and high-order rootchecks are introduced. Finally, different code ensembles are proposed and analyzed for the block-fading channel. Rank deficiency in the LDPC matrix for some type of controlled doping is solved by shortening, or avoided by the use of a simple chain graph. Simulation results are shown for single-antenna and multiple-antenna block-fading channels.

A normal continuation of this work would be a mixing of controlled and uncontrolled doping with irregular degree distributions in order to optimize thresholds with respect to

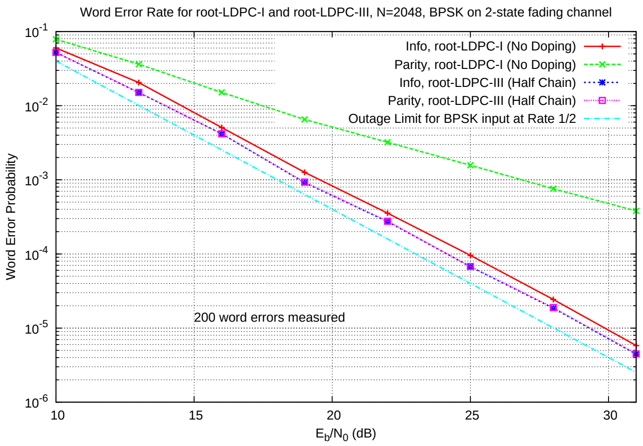


Fig. 9. Root-LDPC-I code versus Root-LDPC-III code on a block-fading channel for code length $N = 2048$ bits. Full diversity corresponds to $d = 2$ in this example.

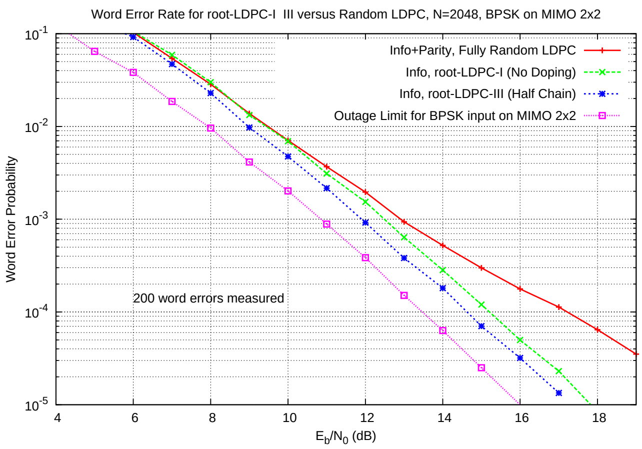


Fig. 10. Root-LDPC-I & III codes versus fully random LDPC on a MIMO 2x2 channel. Similar behavior is observed for both BPSK and QPSK. Full diversity corresponds to $d = 4$ in this example.

the capacity outage boundary in the fading plane. The simple chain example can also be generalized to more elaborated state machines such as time-variant [18] or time-invariant convolutional codes. Finally, for finite length (small and moderate), uncontrolled doping of parity bits also depends on the distribution of stopping sets [19] in the graph. The influence of optimized graphs, such as progressive-edge growth graphs [20], should be investigated.

## Acknowledgement

The author's work was supported by the Broadband Communications Systems project funded by Qatar Telecom (Qtel). The author is also grateful to Mr Wael Halbawi, from Texas A&M University at Qatar, for all nice discussions they had together on low-density parity-check codes.

## References

[1] J.J. Boutros, A. Guillén i Fàbregas, E. Biglieri, and G. Zémor, "Low-density parity-check codes for nonergodic block-fading channels," *IEEE Transactions on Information Theory*, vol. 56, no. 9, pp. 4286-4300, Sept. 2010.

[2] J.J. Boutros, "Diversity and coding gain evolution in graph codes," *Information Theory and Its Applications, ITA'2009*, UCSD, San Diego, California, Feb. 2009.

[3] D.N.C. Tse and P. Viswanath, *Fundamentals of Wireless Communication*, Cambridge University Press, 2005.

[4] T. Richardson and R. Urbanke, *Modern Coding Theory*, Cambridge University Press, 2008.

[5] W.E. Ryan and S. Lin, *Channel Codes: Classical and Modern*, Cambridge University Press, 2009.

[6] J.J. Boutros, G.M. Kraidy, and N. Gresset, "Near outage limit space-time coding for MIMO channels," *Information Theory and Its Applications, ITA'2006*, UCSD, San Diego, California, Feb. 2006.

[7] R. Knopp and P. A. Humblet,"On coding for block fading channels," *IEEE Transactions on Information Theory*, vol. 46, no. 1, pp. 189–205, Jan. 2000.

[8] J. J. Boutros, E. Calvanese Strinati, and A. Guillén i Fàbregas, "Turbo code design for block fading channels," *Allerton Conference on Communication, Control, and Computing*, Monticello, Illinois, Sept. 2004. Downloadable at www.josephboutros.org.

[9] A. Guillén i Fàbregas, "Coding in the block-erasure channel," *IEEE Transactions on Information Theory*, vol. 52, no. 11, pp. 5116-5121, Nov. 2006.

[10] J.J. Boutros, A. Guillen I Fabregas, and E. Calvanese Strinati, "Analysis of coding on non-ergodic block fading channels," *Allertons Conference on Communication, Control, and Computing*, Monticello, Illinois, Sept. 2005 Downloadable at www.josephboutros.org.

[11] J.J. Boutros, G. Zémor, A. Guillén I Fàbregas, and E. Biglieri, "Full-diversity product codes for block erasure and block fading channels," *IEEE Information Theory Workshop*, pp. 313-317, Porto, May 2008.

[12] D. Duyck, "Full-diversity random LDPC ensembles for the block-fading channel," Private Communication, June 2011.

[13] J.J. Boutros, F. Boixadera, and C. Lamy, "Bit-interleaved coded modulations for multiple-input multiple-output channels," *IEEE Sixth International Symposium on Spread Spectrum Techniques and Applications*, vol. 1, pp. 123-126, New Jersey, USA, Sept. 2000.

[14] L. Brunel and J.J. Boutros, "Code division multiple access based on independent codes and turbo decoding," *Annales des Télécommunications*, tome 54, no. 7-8, pp. 401-410, July/August 1999.

[15] R. Kötter, A.C. Singer, and M. Tüchler, "Turbo Equalization," *IEEE Signal Processing Magazine*, vol. 21, no. 1, pp. 67-80, Jan. 2004.

[16] D. Capirone and D. Duyck, "On the rank of root-LDPC matrices," Private Communication, June 2010.

[17] L. R. Bahl, J. Cocke, F. Jelinek, and J. Raviv, "Optimal decoding for linear codes for minimizing symbol error rate," *IEEE Transactions on Information Theory*, vol. 20, pp. 284-287, March 1974.

[18] A. Jiménez Felström and K. Zigangirov, "Time-varying periodic convolutional codes with low-density parity-check matrix," *IEEE Transactions on Information Theory*, vol. 45, no. 6, pp. 2181-2191, Sept. 1999.

[19] C. Di, D. Proietti, I. E. Telatar, T. J. Richardson, and R. L. Urbanke, "Finite-length analysis of low-density parity-check codes on the binary erasure channel," *IEEE Transactions on Information Theory*, vol. 48, no. 6, pp. 1570-1579, June 2002.

[20] X.-Y. Hu, E. Eleftheriou, and D.M. Arnold, "Regular and irregular progressive edge-growth Tanner graphs," *IEEE Transactions on Information Theory*, vol. 51, no. 1, pp. 386-398, Jan. 2005.